Common Digital Identification Project

Anonymous authentication system using Absolute Identifier & Decentralized OTP

아니스트

AHNIST

Network Neutrality Laboratory

Gwon OhGyoung

yalariyala@naver.com

1. Challenge

The need for a global solution for Common Digital Identity

< Difficulty in providing basic welfare due to lack of Identification services in many developing countries >

DIF

fido ALLIANCE simpler stronger authentication

Accountable Digital Identity ADI Association

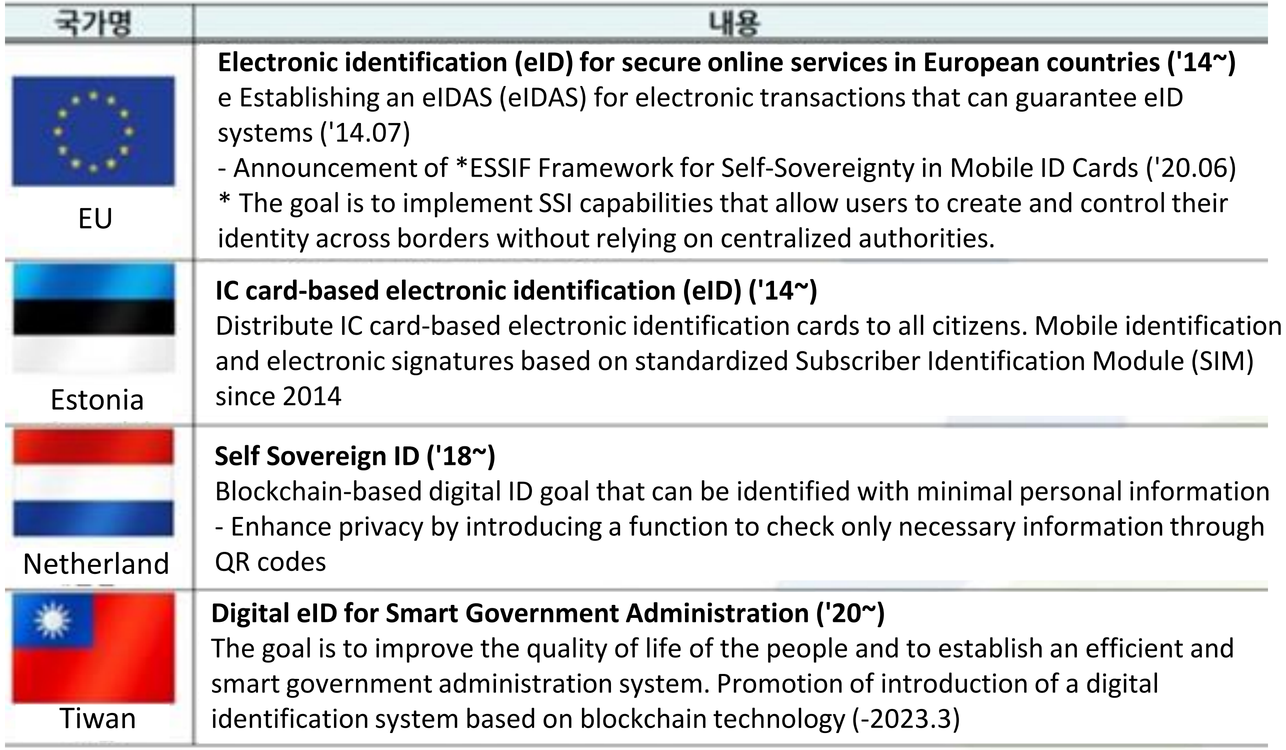
The Commons Project

Gavi The Vaccine Alliance

Many of countries around the world are developing digital Identification system that can be authenticatied globally and introducing them to local governments

[Reference]

Electric Identifier & Vaccine Passport

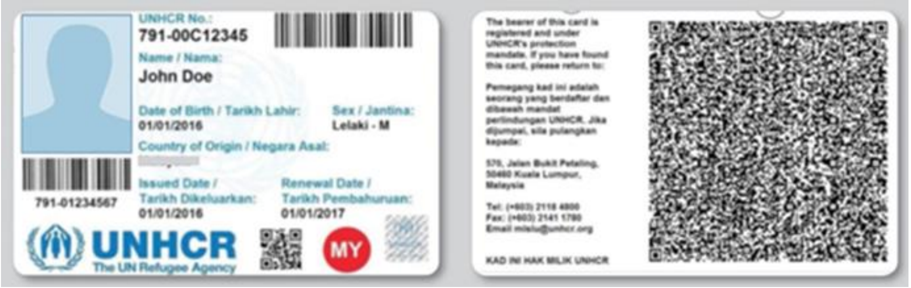


국가명	내용
EU	**Electronic identification (eID) for secure online services in European countries ('14~)** e Establishing an eIDAS (eIDAS) for electronic transactions that can guarantee eID systems ('14.07) - Announcement of *ESSIF Framework for Self-Sovereignty in Mobile ID Cards ('20.06) * The goal is to implement SSI capabilities that allow users to create and control their identity across borders without relying on centralized authorities.
Estonia	**IC card-based electronic identification (eID) ('14~)** Distribute IC card-based electronic identification cards to all citizens. Mobile identification and electronic signatures based on standardized Subscriber Identification Module (SIM) since 2014
Netherland	**Self Sovereign ID ('18~)** Blockchain-based digital ID goal that can be identified with minimal personal information - Enhance privacy by introducing a function to check only necessary information through QR codes
Tiwan	**Digital eID for Smart Government Administration ('20~)** The goal is to improve the quality of life of the people and to establish an efficient and smart government administration system. Promotion of introduction of a digital identification system based on blockchain technology (-2023.3)

[Source : https://www.kisa.or.kr]

< Current progress of Digital Identification System by some countries >

INTERNATIONAL CERTIFICATE OF VACCINATION
THE WORLD HEALTH ORGANIZATION
COVID-19
Certificate ID



UNHCR No.:
791-00C12345
Name / Nama:
John Doe
Date of Birth / Tarikh Lahir:
01/01/2016
Sex / Jantina:
Lelaki - M
Country of Origin / Negara Asal:
791-01234567
Issued Date / Tarikh Dikeluarkan:
01/01/2016
Renewal Date / Tarikh Pembahuruan:
01/01/2017

The bearer of this card is registered and under UNHCR's protection mandate. If you have found this card, please return to:

Pemegang kad ini adalah seorang yang berdaftar dan dibawah mandat perlindungan UNHCR. Jika dijumpai, sila pulangkan kepada:

570, Jalan Bukit Petaling,
50460 Kuala Lumpur,
Malaysia

Tel: (+603) 2118 4800
Fax: (+603) 2141 1780
Email: mislu@unhcr.org

KAD INI HAK MILIK UNHCR

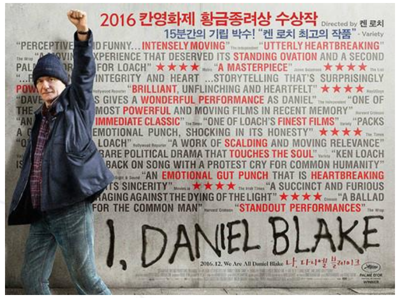
Various certificate and verify services based on smart devices are flooding due to the covid-19 crisis

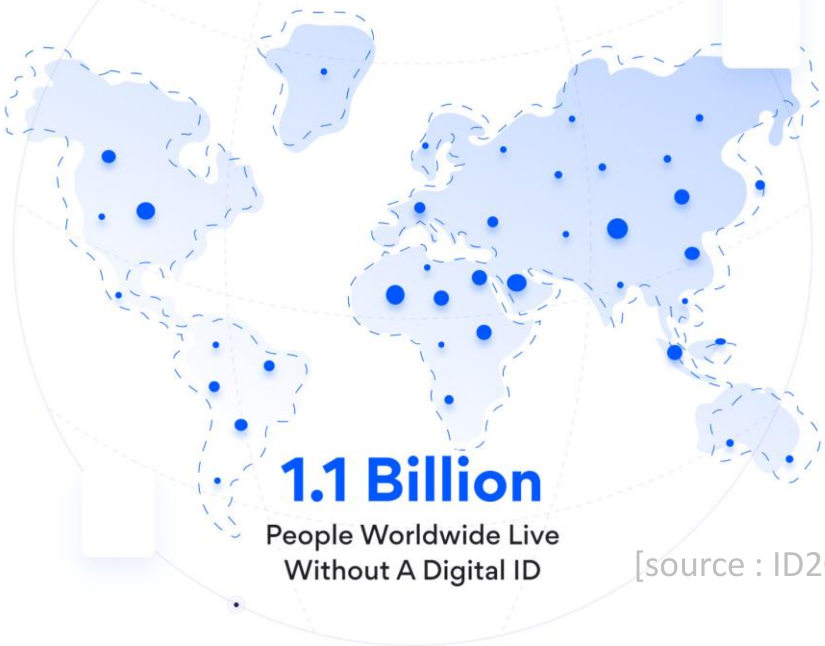
2. Problem

Human Rights alienation due to Legacy Identity Systems

< Myanmar's citizens staging peaceful protests against the government forced into power in a military coup >

*** I, Daniel Blake (2016, 100min)**
A film directed by Ken Roach. The film is set in Newcastle, England, and features criticism of the modern welfare system.





[source : ID2020.org]

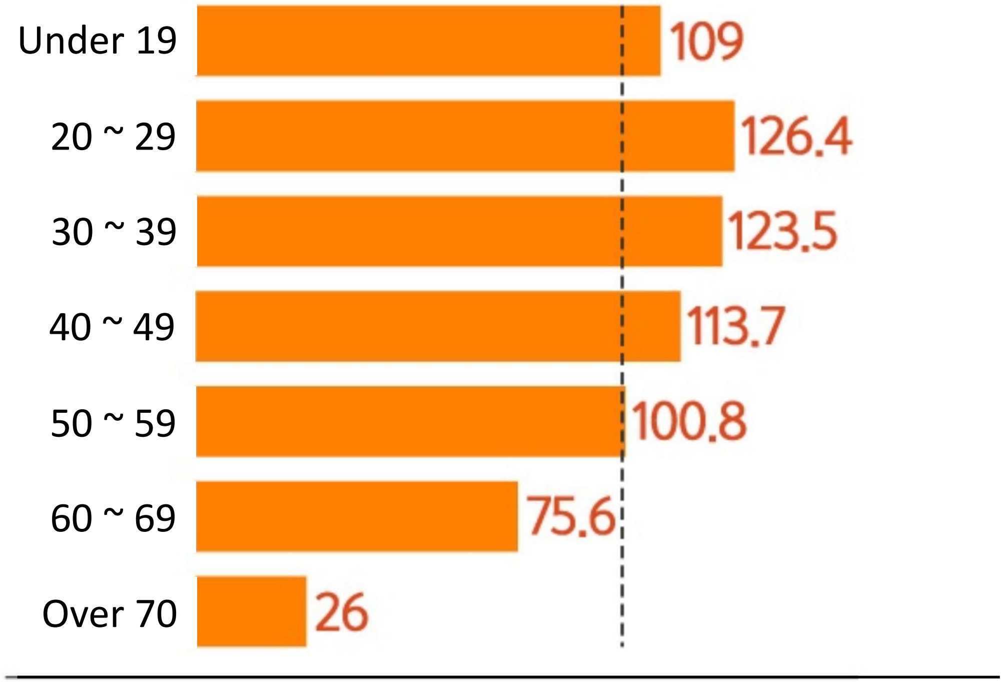
[Reference]

No Identity solution for Underprivileged Commons

< Hong Kong's civil movement, faced with limitations due to sanctions through the legal identity system >

Digital availability status by Age group

(average of total : 100%)



[Source : https://www,nia.or.kr]

[Insight]

Requirements of Common Digital Identity

1. Easy to use including Senior, Poor and Disabled People

2. Strictly distinguish between Public and Private Usability

3. Self-Sovereign authenticate without Established Forces

3. Solution [1/3]

* : New word

*AID : Absolute Identifier

[Level 1] Security Key

Electric Card

USB Key

[Level 2] Security Storage

USB Storage

Cold Wallet

[Level 3] Node Device (TEE Support)

Smart Phone

PC

NAS

[Reference] FIDO2 (WebAuthn + CTAP)

Not only does it provide basic identity authentication for smart devices, but it also provides the use of web services supported by WebAutn through an external certification system called CTAP. Unlike AID, which plays an absolute role, there is a difference that CTAP is an auxiliary role for FIDO servers.

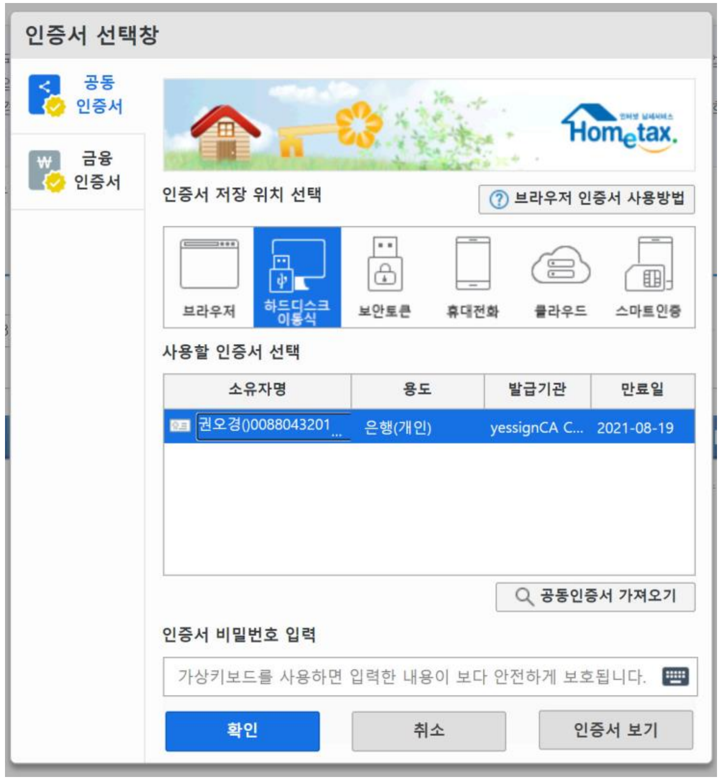
refer to : fido ALLIANCE

※ TEE(Trusted Excution Enviroment) :

A security system that combines hardware and software. Independent OS-driven environment with strict levels of security, such as identity authentication, in CPU areas where external access is not available

[Method]

Activation scheme using Credential Data



인증서 선택창

인증서 저장 위치 선택

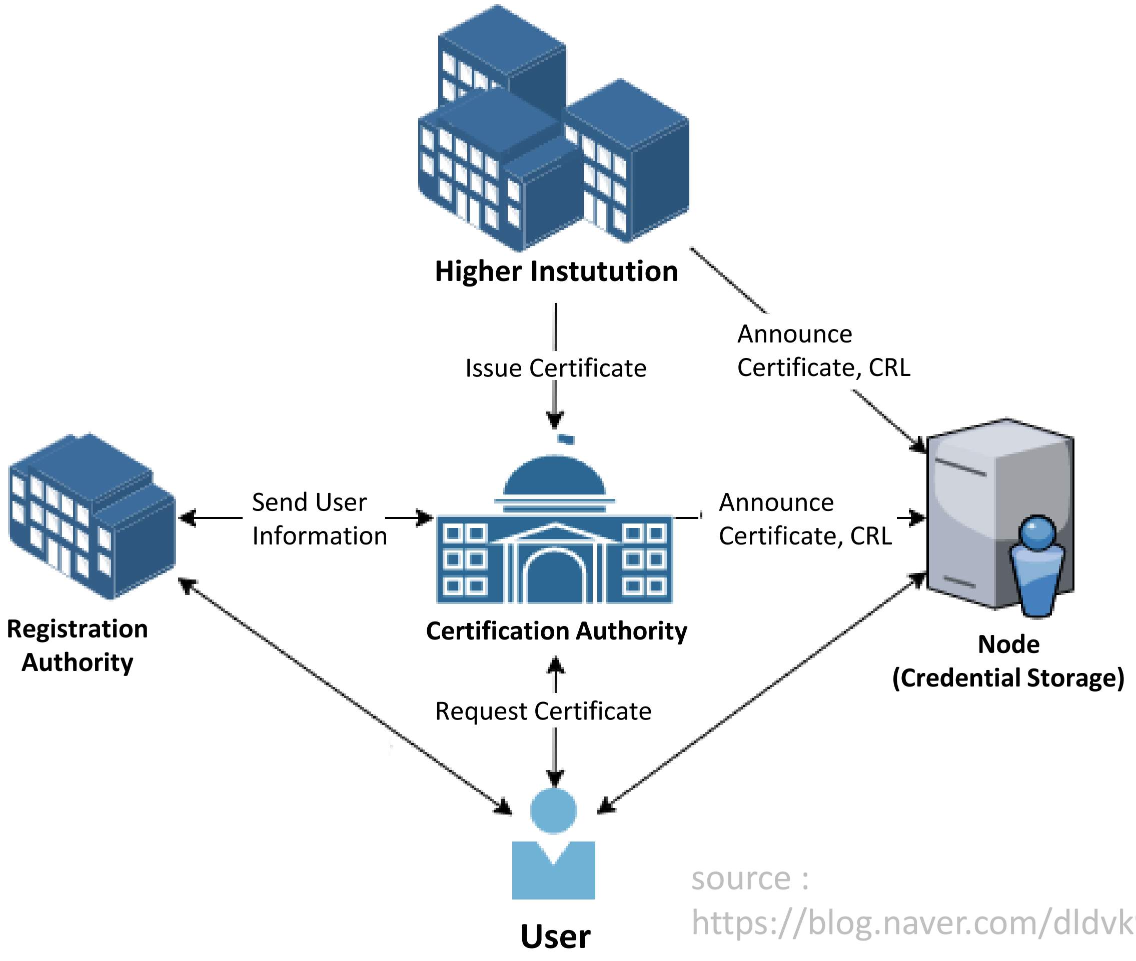
사용할 인증서 선택

소유자명	용도	발급기관	만료일
권오경()0088043201...	은행(개인)	yessignCA C...	2021-08-19

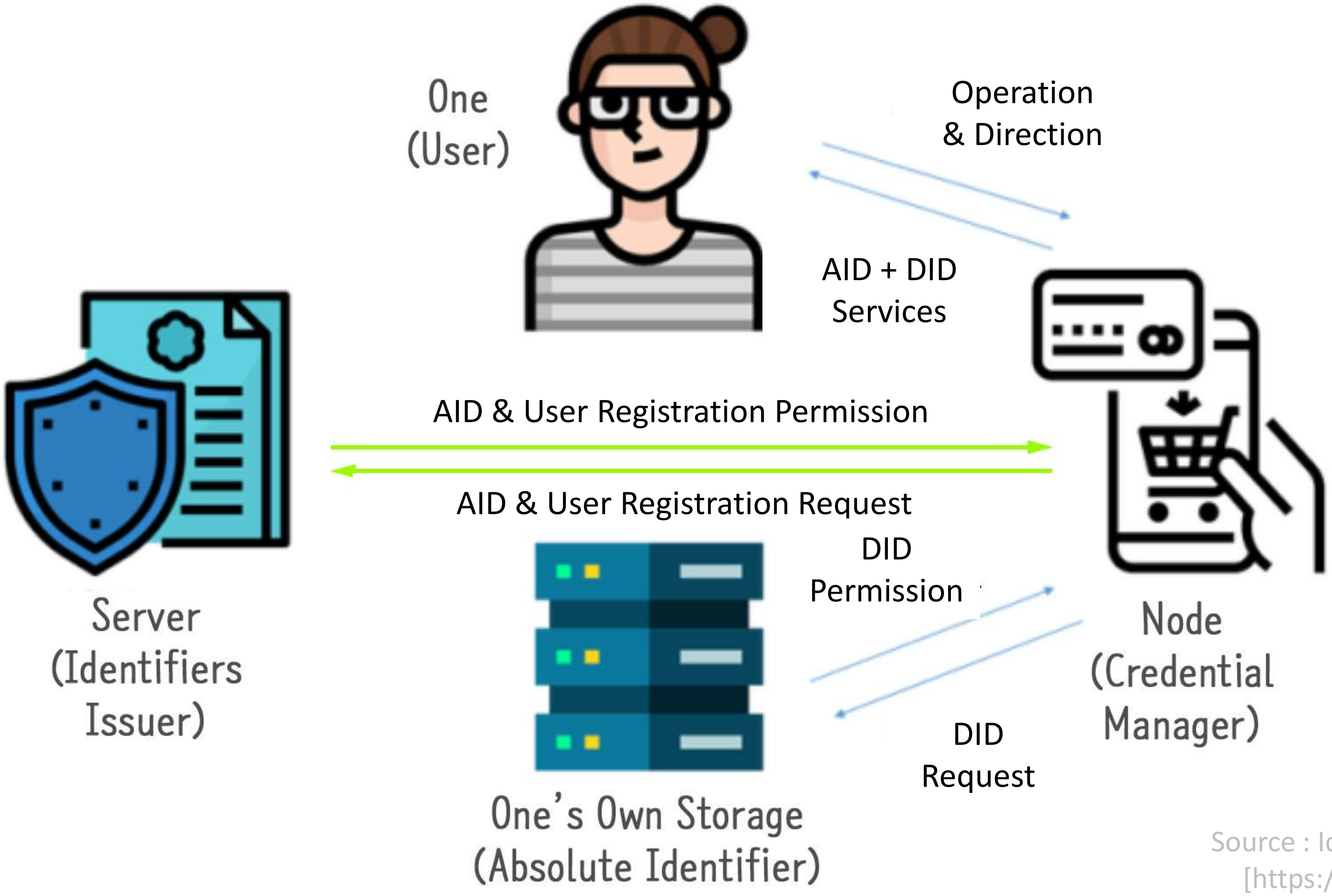
인증서 비밀번호 입력

가상키보드를 사용하면 입력한 내용이 보다 안전하게 보호됩니다.

< Authorized certificate Legal permitted
to use private companies in South Korea >



source : https://blog.naver.com/dldvk9999

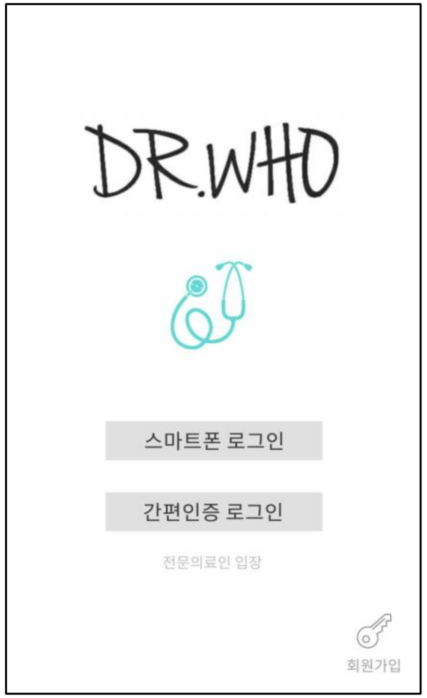


Source : Icon made by monkik
[https://www.flaticon.com]

< Authentication scheme of Credential Data and DID using AID >

1. Authenticator : AID

2. Agent : Node

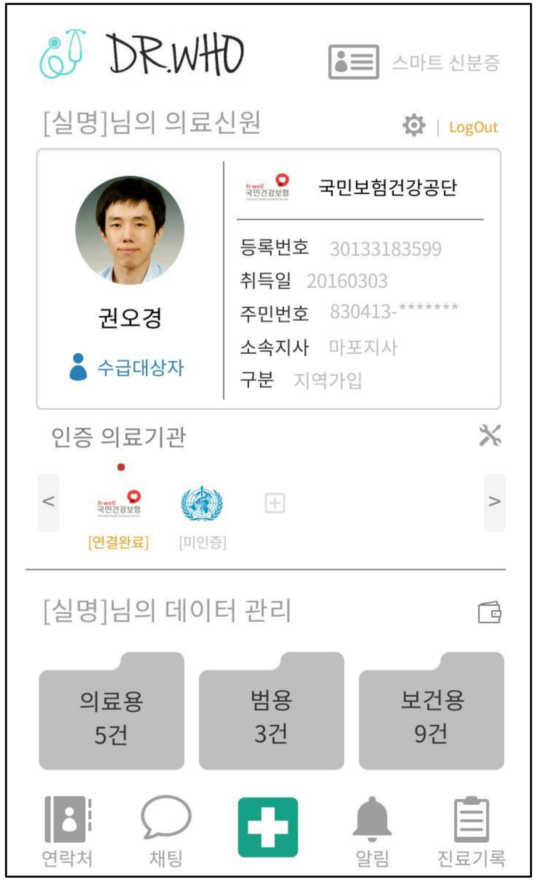


3. Verifier : Application

→ Authenticate the **AID as a Subject**, Verify the **Node as an Agent**

3. Solution [2/3]

Mobile Platform : Self-Sovereign Credential Manager



DR.WHO

스마트 신분증

[실명]님의 의료신원

LogOut

권오경

수급대상자

국민보험건강공단

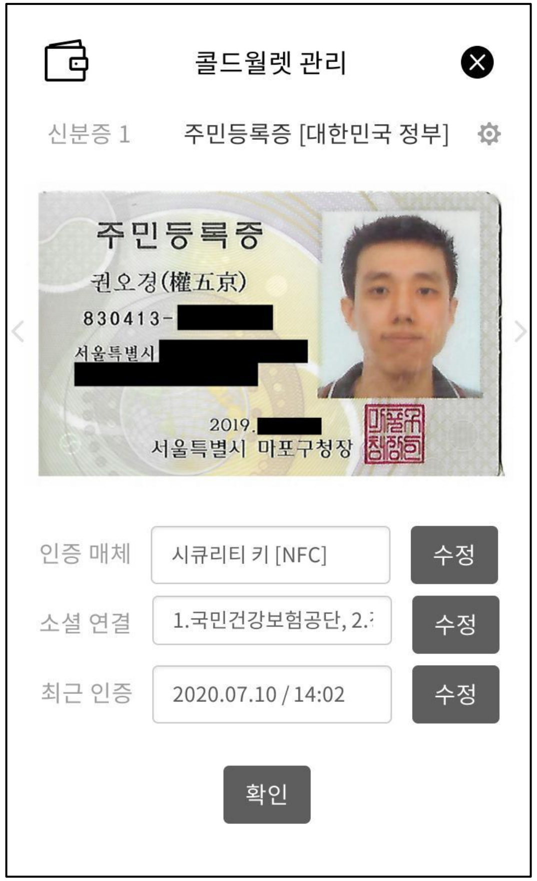
등록번호	30133183599
취득일	20160303
주민번호	830413-*******
소속지사	마포지사
구분	지역가입

인증 의료기관

[연결완료] [미인증]

[실명]님의 데이터 관리

의료용 5건	범용 3건	보건용 9건



콜드월렛 관리

신분증 1　주민등록증 [대한민국 정부]

주민등록증

권오경(權五京)

830413-[redacted]

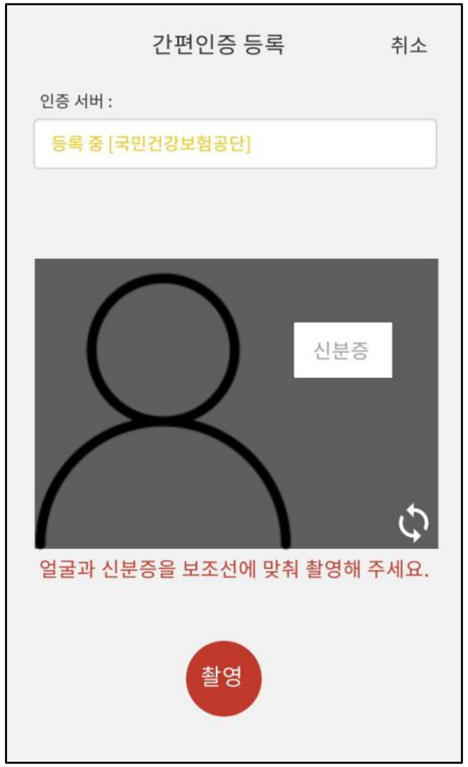
서울특별시 [redacted]

2019.[redacted]

서울특별시 마포구청장

인증 매체	시큐리티 키 [NFC]	수정
소셜 연결	1.국민건강보험공단, 2.	수정
최근 인증	2020.07.10 / 14:02	수정

확인

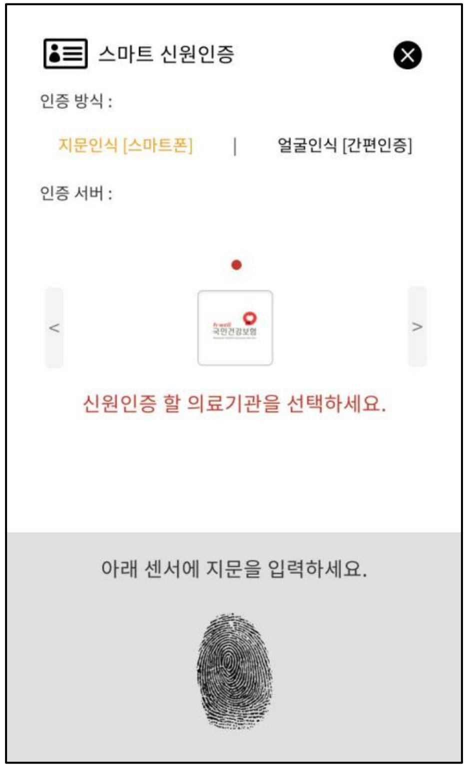


간편인증 등록　취소

인증 서버 : 등록 중 [국민건강보험공단]

얼굴과 신분증을 보조선에 맞춰 촬영해 주세요.

촬영



스마트 신원인증

인증 방식 : 지문인식 [스마트폰] | 얼굴인식 [간편인증]

인증 서버 :

신원인증 할 의료기관을 선택하세요.

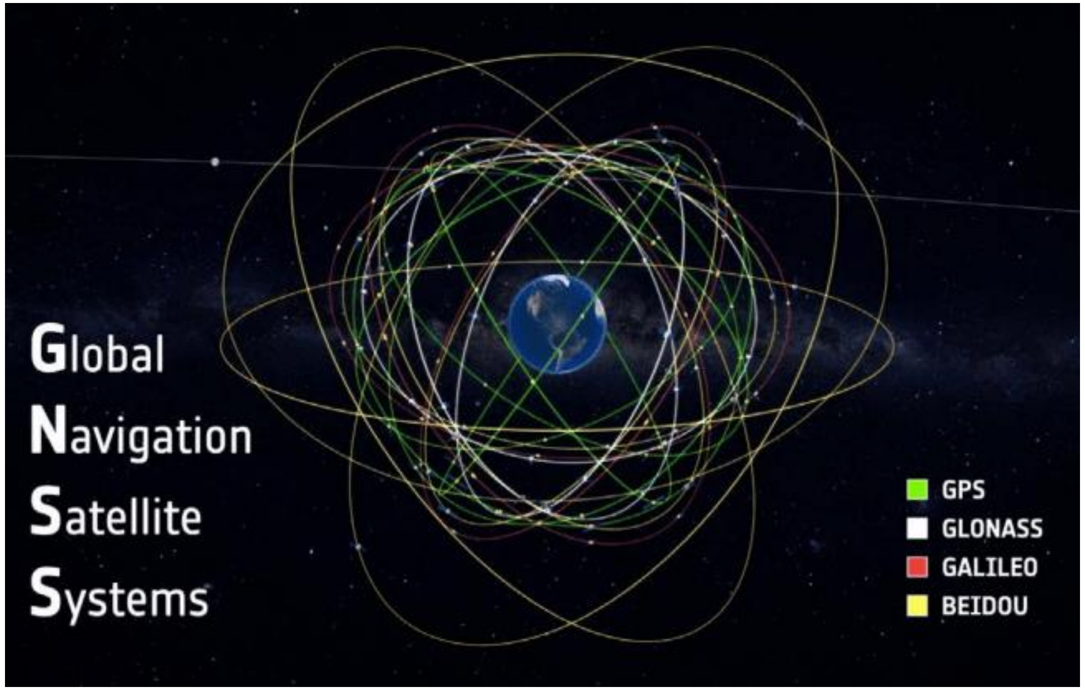
아래 센서에 지문을 입력하세요.

< UI/UX draft for Personal medical Authentication App >

[Manual]

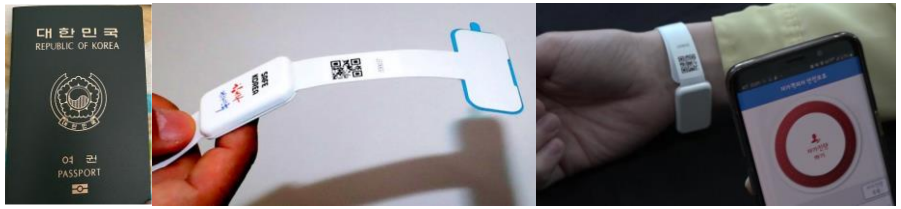
* : New word

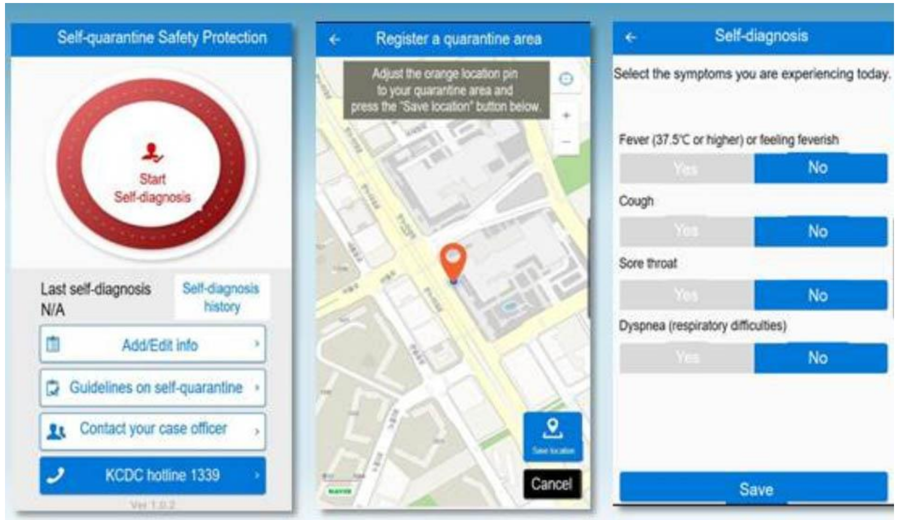
*PoE : Proof of Existence



< Status of Global Navigation Satellite System(GNSS) >

※ SBAS(Satellite Based Augmentation System) :
A System that support more precise measurements of GNSS through ground station reinforcement signals.





Self-quarantine Safety Protection

Start Self-diagnosis

Last self-diagnosis
N/A

Self-diagnosis history

Add/Edit info

Guidelines on self-quarantine

Contact your case officer

KCDC hotline 1339

Register a quarantine area

Adjust the orange location pin to your quarantine area and press the "Save location" button below.

Save location

Cancel

Self-diagnosis

Select the symptoms you are experiencing today.

Fever (37.5℃ or higher) or feeling feverish
Yes [✓ No]

Cough
Yes [✓ No]

Sore throat
Yes [✓ No]

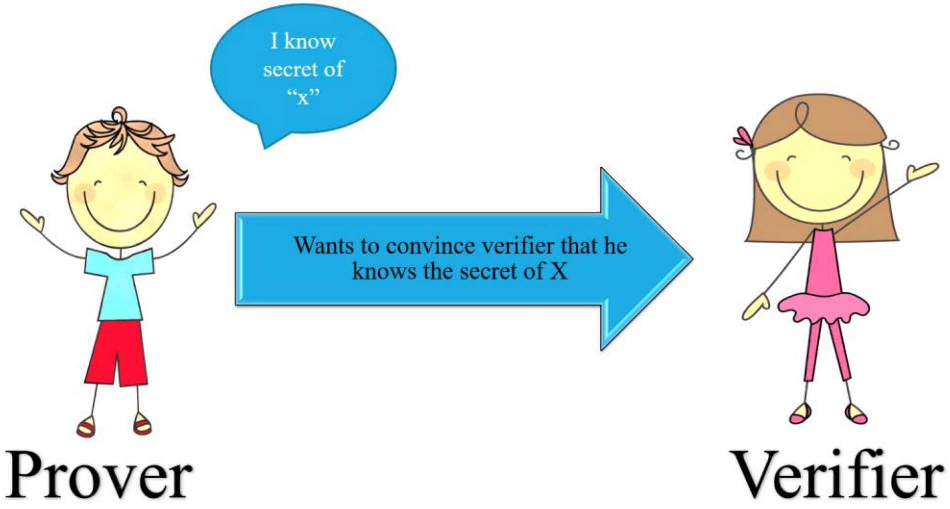
Dyspnea (respiratory difficulties)
Yes [✓ No]

Save

Record Location info and Time values based-on One's own AID & Node
(False Screening through Integrity Check)

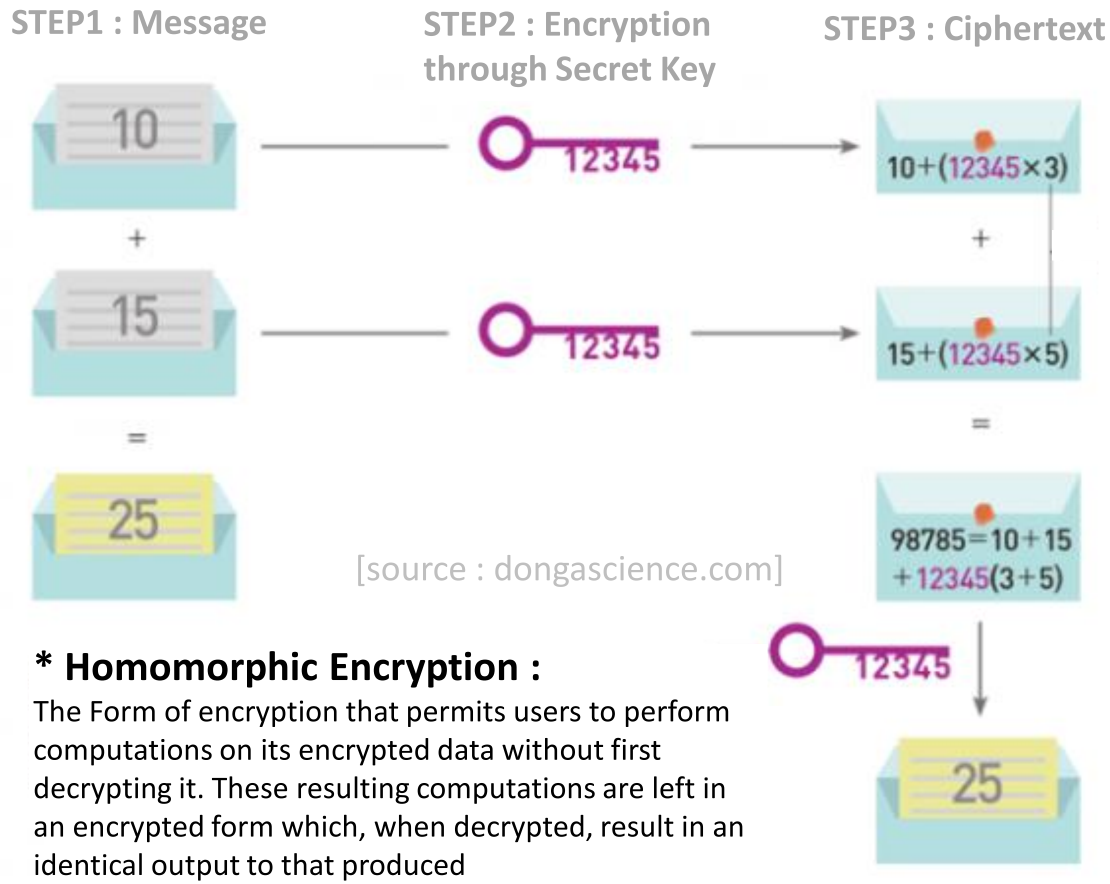
[Method]

Utilization of Anonymous through End-to-End Encryption



[source : Dhruvil Kotecha, zero knowledge proof]

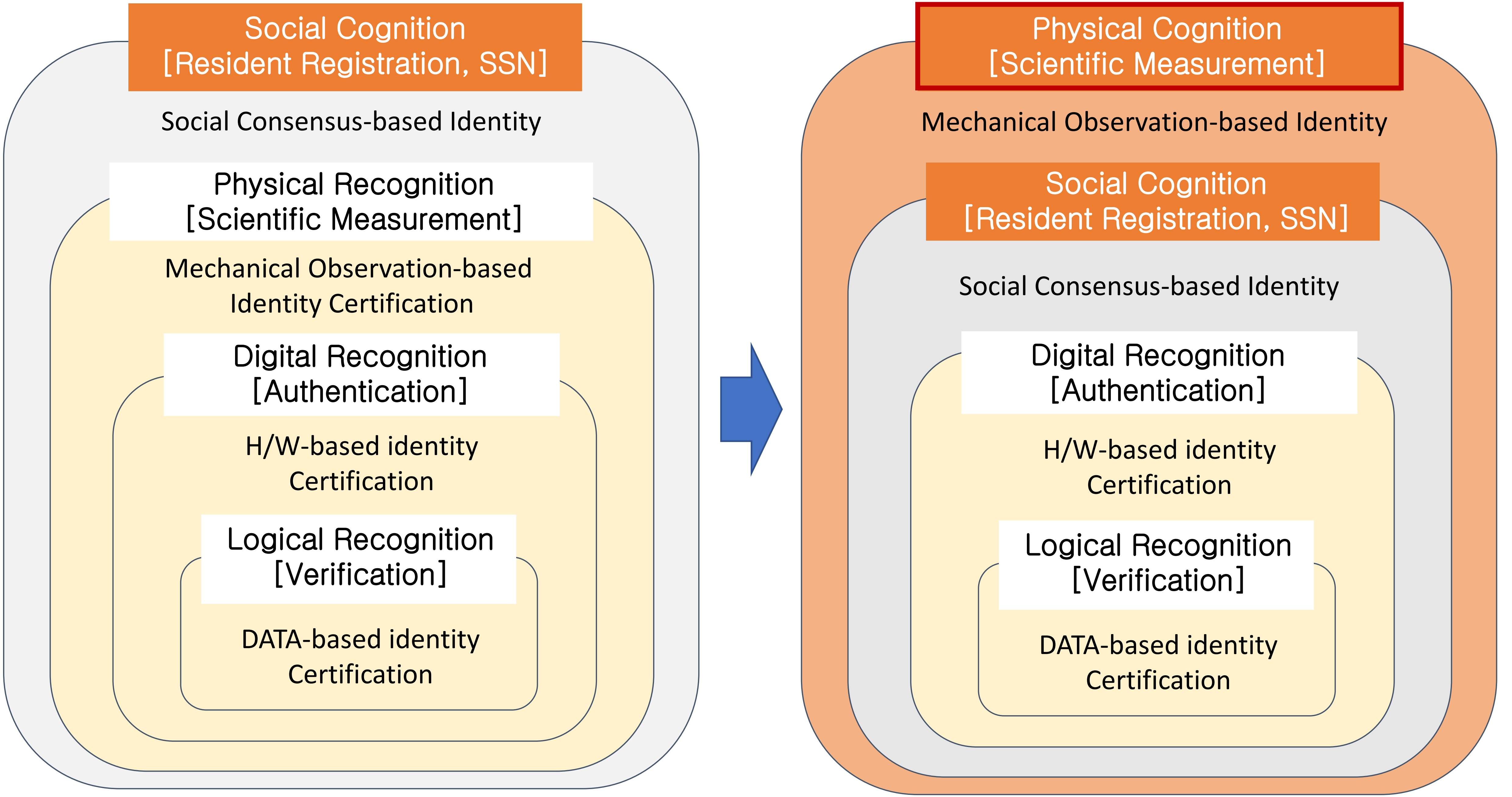
< Public service need to de-identification of personal information on platform server >



[source : dongascience.com]

*** Homomorphic Encryption :**

The Form of encryption that permits users to perform computations on its encrypted data without first decrypting it. These resulting computations are left in an encrypted form which, when decrypted, result in an identical output to that produced



< Legacy Identity Cogniton & Identification Scheme >

< Improved Identity Cognition & Identification Scheme >

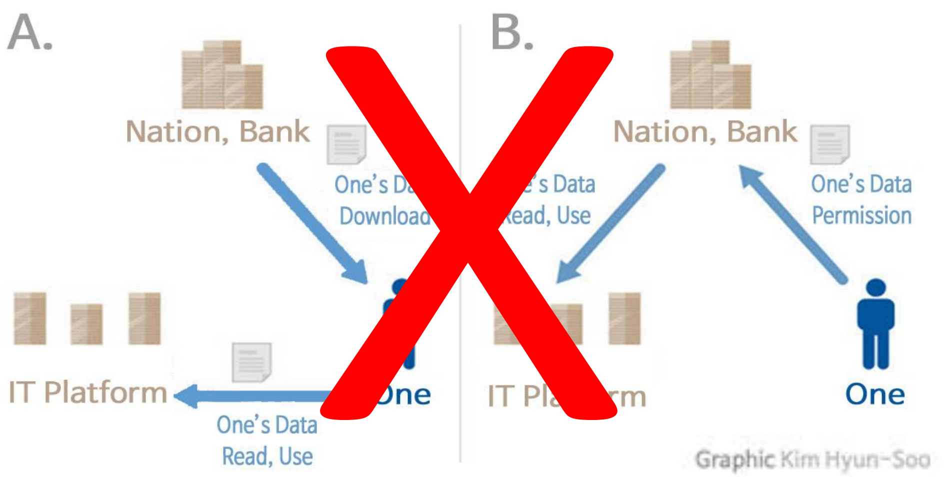
3. Solution [3/3]

* : New word

* D-OTP : Decentralized One Time Password

[Reference] CGD(Chip Guard Display) Card

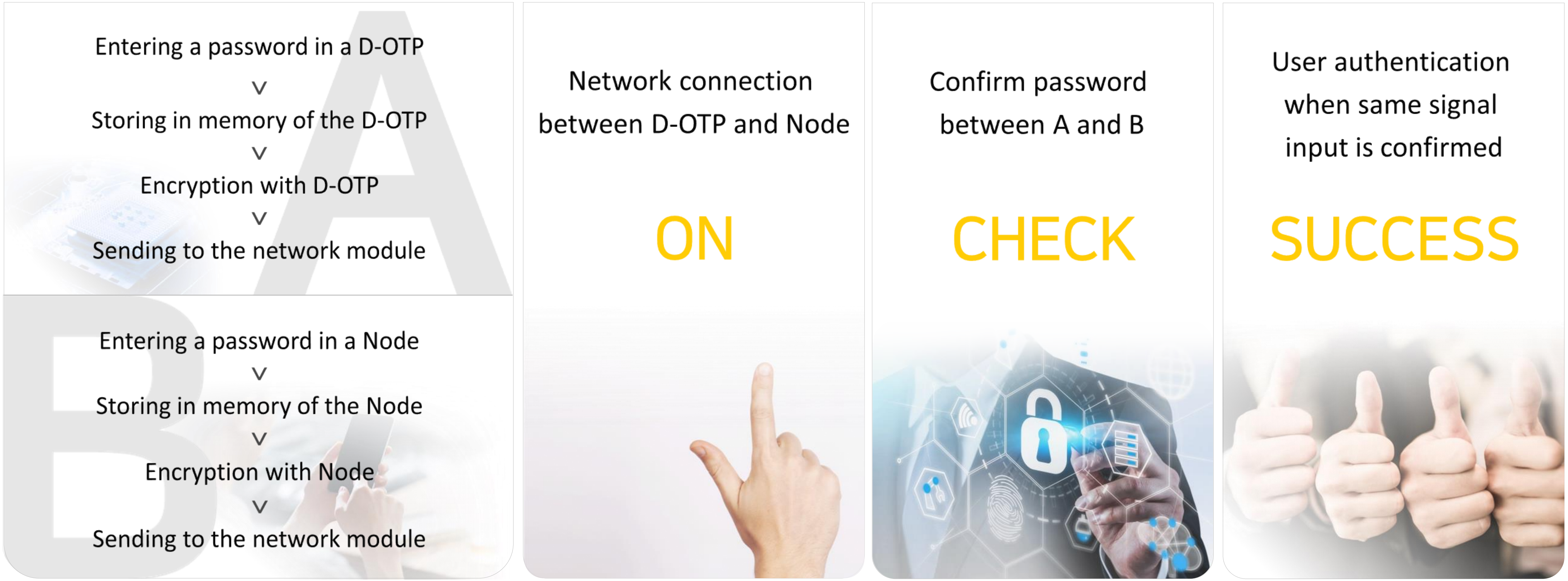
It was expected to be a future authentication alternative to OTP, but it follows existing central custody approaches. And It also failure to differentiated usability and secure proper durability has led to be eliminated in the market.



[NOTICE] Owner of AID must be same as the node, and not delegate his or her authority to the others

[Manual]

Self-Sovereign Exercise Authentication



Entering a password in a D-OTP
V
Storing in memory of the D-OTP
V
Encryption with D-OTP
V
Sending to the network module

Entering a password in a Node
V
Storing in memory of the Node
V
Encryption with Node
V
Sending to the network module

Network connection
between D-OTP and Node

ON

Confirm password
between A and B

CHECK

User authentication
when same signal
input is confirmed

SUCCESS

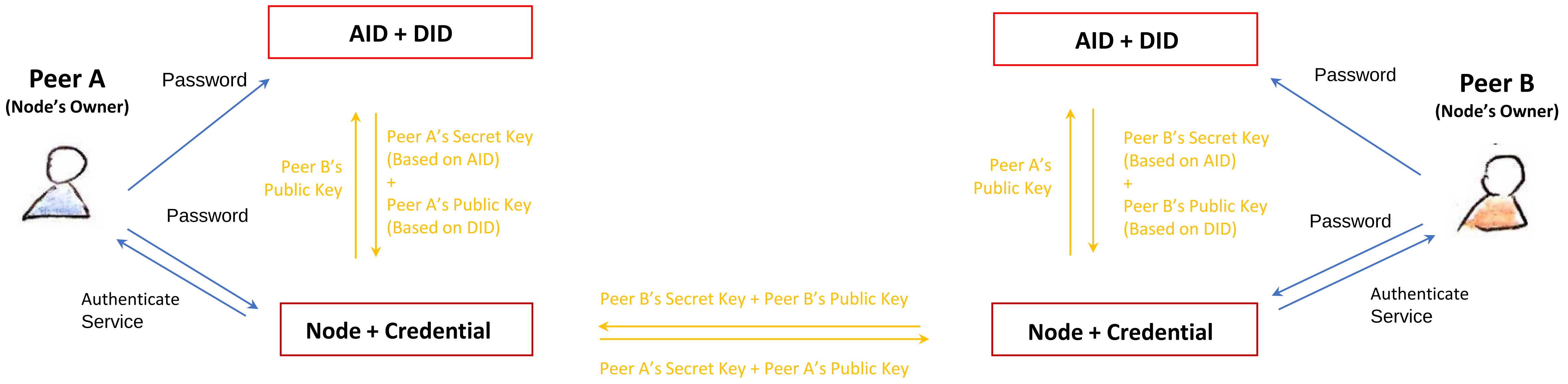
※ It doesn't matter which process A or B goes first.

[Workflow 1]

Private

* Computation of Node A
1. Confirm password between AID and NODE
2. Checking AID registered with a server
3. Issue above-based Secret Key, Public Key
4. the others Secret Key, Public Key decryption

* Computation of Node B
1. Confirm password between AID and NODE
2. Checking AID registered with a server
3. Issue above-based Secret Key, Public Key
4. the others Secret Key, Public Key decryption



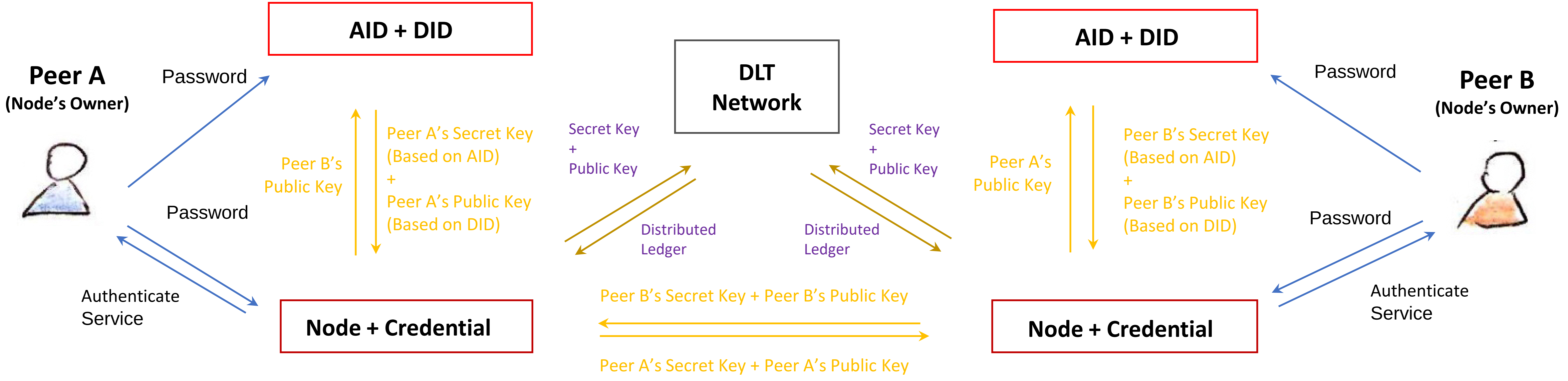
[Workflow 2]

Public

* Computation of Node A
1. Confirm password between AID and NODE
2. Checking AID registered with a server
3. Issue above-based Secret Key, Public Key
4. the others Secret Key, Public Key decryption

* Computation of DLT Network
1. Check the AID information of each nodes
2. Confirm transaction integrity of each nodes
3. Register transaction of distributed ledgers

* Computation of Node B
1. Confirm password between AID and NODE
2. Checking AID registered with a server
3. Issue above-based Secret Key, Public Key
4. the others Secret Key, Public Key decryption



Peer A
(Node's Owner)

Password

Password

Authenticate
Service

AID + DID

Peer B's
Public Key

Peer A's Secret Key
(Based on AID)
+
Peer A's Public Key
(Based on DID)

Node + Credential

DLT
Network

Secret Key
+
Public Key

Distributed
Ledger

Secret Key
+
Public Key

Distributed
Ledger

Peer B's Secret Key + Peer B's Public Key

Peer A's Secret Key + Peer A's Public Key

AID + DID

Peer A's
Public Key

Peer B's Secret Key
(Based on AID)
+
Peer B's Public Key
(Based on DID)

Node + Credential

Password

Peer B
(Node's Owner)

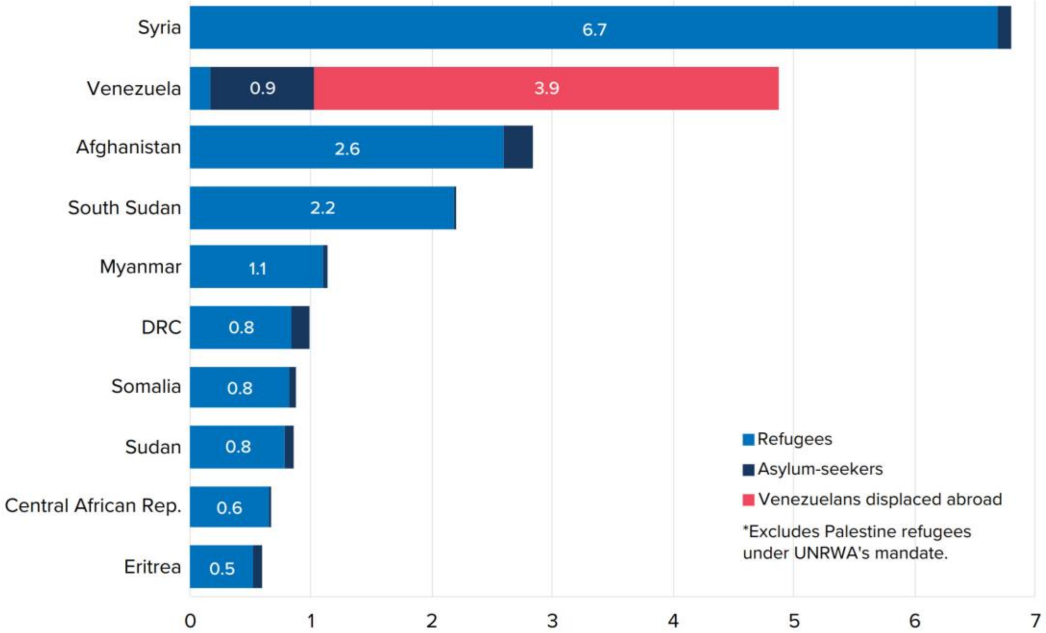
Password

Authenticate
Service

[Social Effect 1]

Refugee

< Loss of identity due to war, coups, political issues, etc >



UNHCR
The UN Refugee Agency

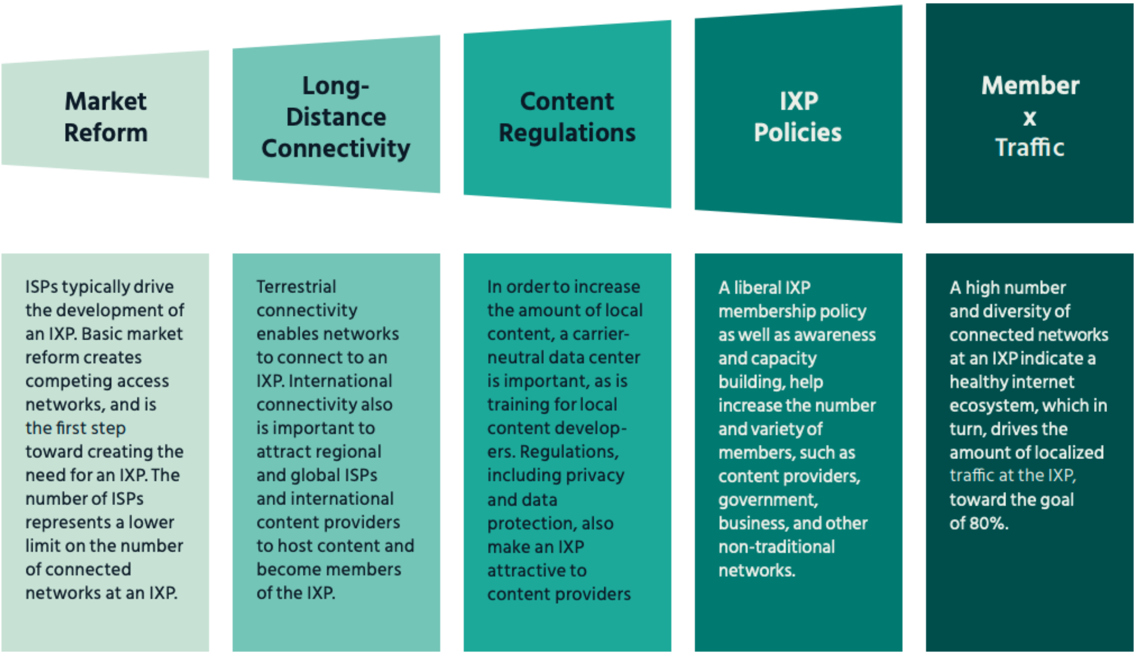
Source : UN HCR(end-2020)

< displacement situations by country of origin >

[Social Effect 2]

Poor, Outcast

World Food Programme(WFP) : The food-assistance branch of the United Nations. It is the world's largest humanitarian organization, the largest one focused on hunger and food security, and the largest provider of school meals. Founded in 1961, it is headquartered in Rome and has offices in 80 countries.



Market Reform	Long-Distance Connectivity	Content Regulations	IXP Policies	Member x Traffic
ISPs typically drive the development of an IXP. Basic market reform creates competing access networks, and is the first step toward creating the need for an IXP. The number of ISPs represents a lower limit on the number of connected networks at an IXP.	Terrestrial connectivity enables networks to connect to an IXP. International connectivity also is important to attract regional and global ISPs and international content providers to host content and become members of the IXP.	In order to increase the amount of local content, a carrier-neutral data center is important, as is training for local content developers. Regulations, including privacy and data protection, also make an IXP attractive to content providers	A liberal IXP membership policy as well as awareness and capacity building, help increase the number and variety of members, such as content providers, government, business, and other non-traditional networks.	A high number and diversity of connected networks at an IXP indicate a healthy internet ecosystem, which in turn, drives the amount of localized traffic at the IXP, toward the goal of 80%.

Though half the countries in Africa have IXPs, a great majority are yet to boost the levels of Internet traffic that is locally exchanged from 20% to 80%. The following enablers can foster change

[Source: internetsociety.org]

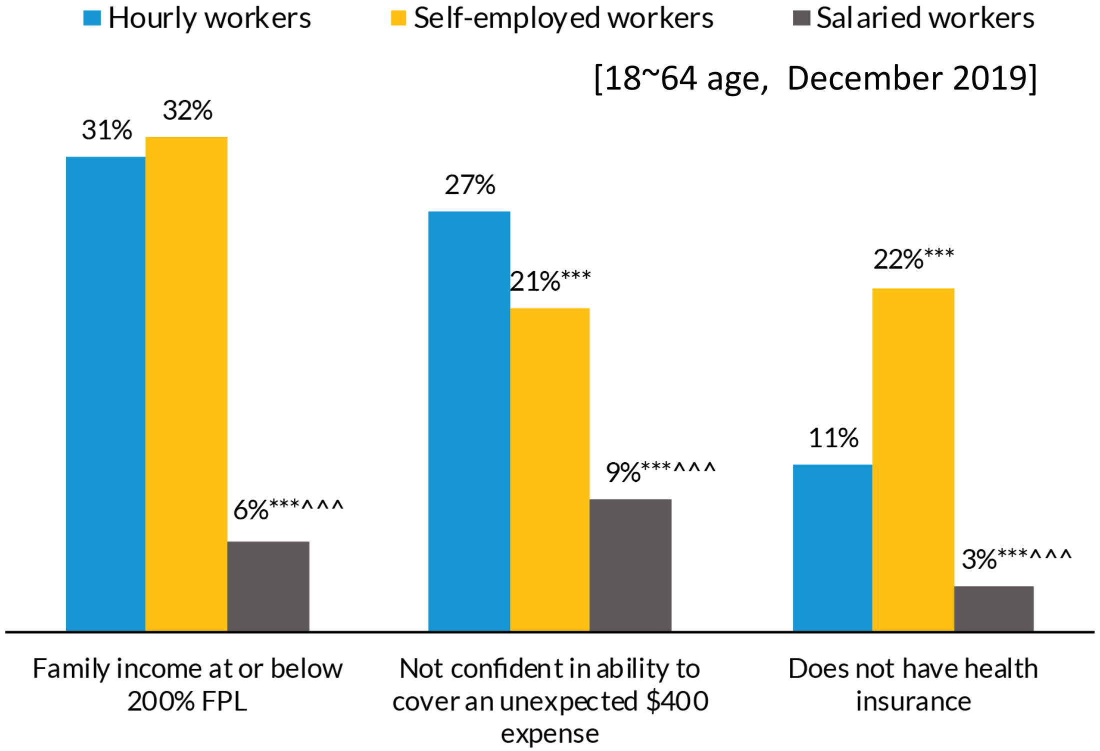
[Social Effect 3]

Nomad, Anarchist

Indie band : Artist group producing independently from commercial record labels or their subsidiaries, who do-it-themselves perform to recording and publishing.

NGOs : Activist group are usually non-profit organizations, and many of them are active in humanitarianism or the social sciences in independent of government involvement

[Source : wikipedia.org]



[18~64 age, December 2019]

< Independant people such as Self-employed, Free-agent >

[Source : urban.org, ‘Well-being and Basic Needs Survey’]

4. Ecosystem

Technology Forum of Self-Sovereign Identity

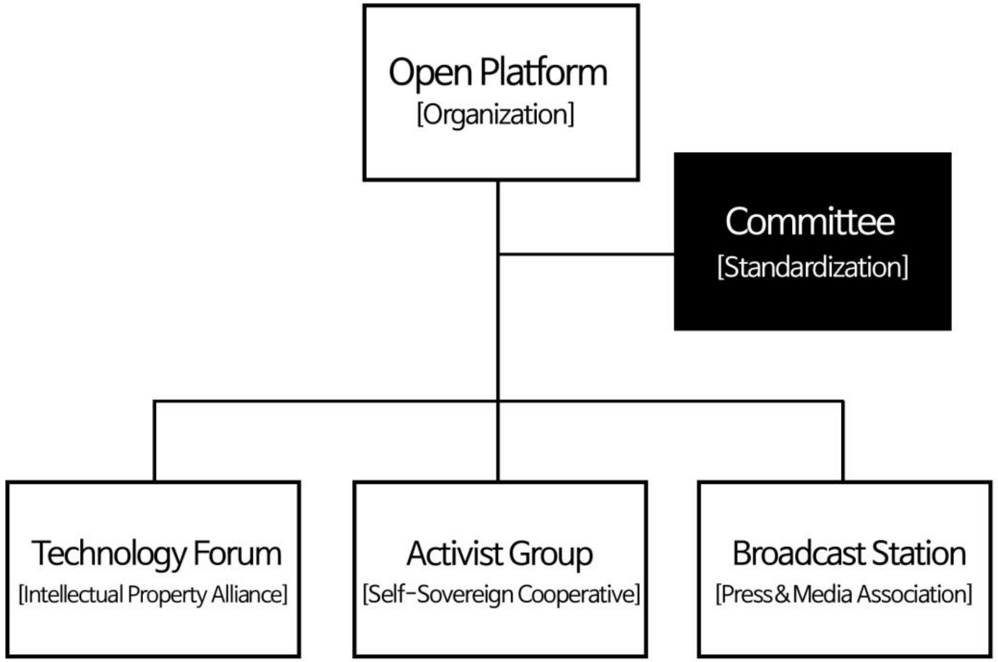
- Establishment of technical standards for certification based on Self-Sovereign Identity, operation and management of public servers

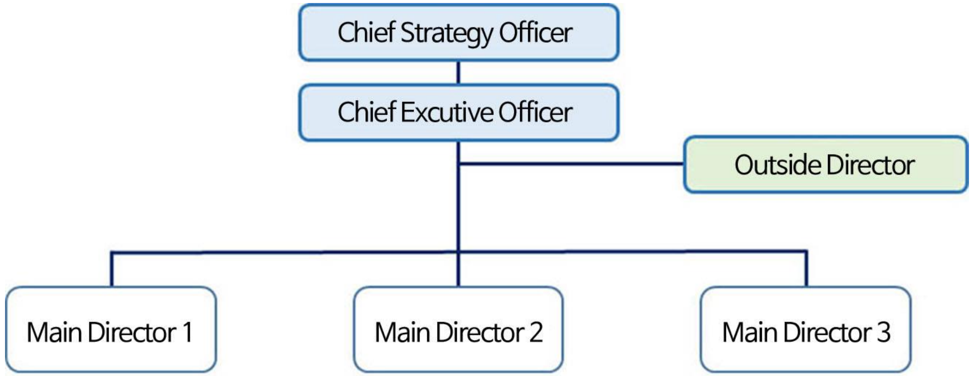
- Development recommendations for Absolute Identifier(AID) prototyping, technical partnership, and development recommendations

- Technology patent, trademark acquisition and linked operation strategies, and license issuance

[Organization]

Public Offer : Patent only free for joining the Organization or subsidiary





A. Intellectual Property Alliance : Provide and Charge Intellectual Property service and server certification by each platforms

B. Self-Sovereign Cooperative : Donates more than 50% of business revenue to Holding Foundation as a income deduction

C. Press & Media Association : Paying each cooperative member salary and bonus according to their history of evaluation system

Now on Sale : bellow Licenses of patents

* TITLE : IDENTIFICATION DEVICE

- Application number : KR/10-2021-0050963

* TITLE : CONTENTS WALLET APPARUTUS AND SELF-SOVEREIGN IDENTITY AND COPYRIGHT AUTHENTICATION SYSTEM USING THE SAME

- PCT number : KR2020/016341 **- Registration number : KR/10-2288971**

- Application number : US/17/617,418

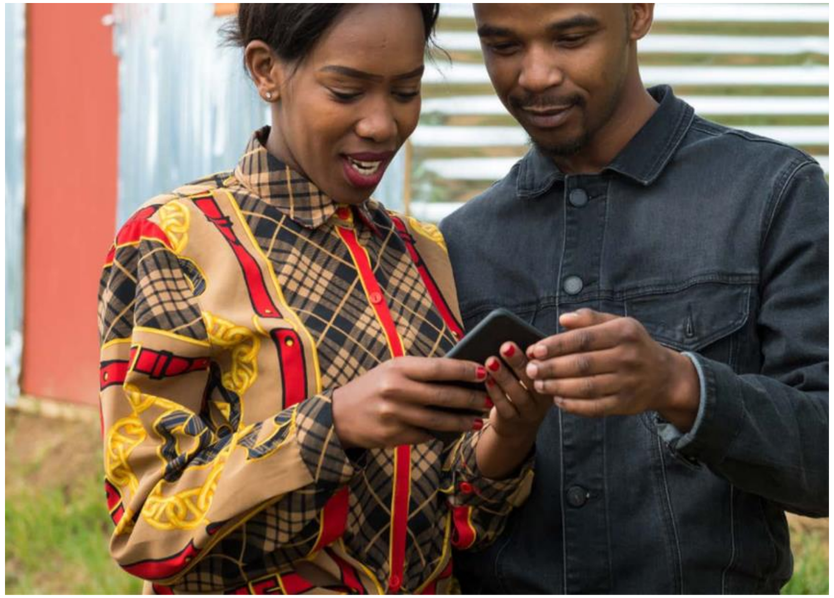
Common Digital Identity for Most People

World Health Organization

unicef
for every child

KOICA
Korea International Cooperation Agency

WORLD BANK



- Modify and supplement to include most developing country

- Partnerships with Global NGO, NPO and Public Funds

Digital identity authentication system available to

most people around the world

Thank you

http://www.ahnist.com